Designing for Safety trumps Operability
A Case Study at Sizewell B

Bryan Coxson
EDF Energy
Generation: Design Authority
Lessons Learnt from Simulator Studies at Sizewell B

- SZB PSA Team (at Barnwood) got involved in 2009

- Classic (vanilla flavour) scenarios studies
  - SGTR, Bleed & Feed, Loss Of Offsite Power (LOOP)

- Study of LOOP with 2 out of 4 EDGs unavailable, run in 2011
  - Demanding on operators – Battery Charging DGs need local start
Burden on the Operators

• “We need to get an Op Tech out promptly on plant to do a CATS Reset before the compressors trip”

• Aim is to prevent an air pressure drop in the Clean Air Trains System (CATS)
  - otherwise the dump valve opens, and CATS depressurises

• All air-operated CATS valves go to fail-safe state
  - unless backed by the Nitrogen system
Lessons Learned (by SZB PSA Team)

• Talk to Operators and do scenario studies to find out:
  - What Operators actually do
  - What they perceive to be important (e.g. retain control of plant)
  - What else they have to do, as well as the Operator action in the PSA
Three Mile Island Control Room
Response by US Nuclear Industry following TMI

• Institute of Nuclear Power Operations set up in 1979 following Three Mile Island Accident
  - A recommendation in Kemeny Commission Report
  - An institute funded by nuclear utilities, but independent of them

• Its missions include
  - Promoting operational excellence
  - Improving Feedback of Operational Experience (OE) between US nuclear operators
US Nuclear Operational Experience (OE)

• A lot of OE in 1970s (and 1980s) was on instrument air, and air operated valves
  - INPO SERs & SOERs
  - US NRC NUREGs & GLs
  - Nuclear Safety Advisory Centre (EPRI) reports

• Two main concerns:
  - Gradual declining air pressure
  - Contamination
Instrument Air Problems – Effect on Nuclear Plant

- Both concerns can put plant into an “unanalysable state”
- Gradual decline in air pressure: Can’t predict the sequence of valves moving to fail-safe state
  - Causes:
    - Compressor failures, or Electrical Board failures
- Contamination: valves stick or operate spuriously
  - Causes:
    - Moisture, Corrosion products, Oil, Hydrogen, Dessicant powder
Meanwhile, what was happening in the UK?

- **Wedding of Charles and Diana – July 1981**
  - After Vows Fluffed
  - Kettles turned on
  - A major grid system pick up

- **Miners Strike 1984-1985**
  - No major blackouts
  - Nuclear power helped
And in the UK Nuclear Industry…

- **AGR’s**
  - Major delays in building and commissioning
  - Were failing to achieve their output design targets
- **PWR technology transfer into the UK**
  - Sizewell B public inquiry started 1982
    - with Frank Layfield as inspector
  - Inspector’s 3,000 page report issued 1987
    - after record breaking inquiry

**SZB Project is going to build to time and cost!**
The UK PWR Designer’s Problem

• UK regulator (NII) reluctant to see numerical credit taken for qualitative improvements unless there is evidence:
  - US (LWR NPPs) or UK (CEGB) data?

• Argued by SZB Project that SZB’s “peer group” was the US PWRs

• Process used by SZB Project to consider “Design Implications” of (mainly US) Operational Experience
Common Mode Failure (CMF) Considerations

  - Spawned various “Guidance” documents

- Resulted in stakeholder expectations (including NII)
  - Design should incorporate diversity systematically
  - System Cut-offs should limit reliability claims

  Unless Operational Experience could justify better
  - it usually couldn’t do at that time
Waiting for Consent

• SZB project finally got go ahead in 1987
  - and was “a more mature design”
• SZB design, compared with reference plant, now had some additional systems
  - EBS, ECS, RUHS, Double Containment
• Extensive changes within many systems
• Design used by Westinghouse and Nuclear Electric in joint bid in 1995 for Taiwan Lungmen plant
  - As met EPRI Advanced LWR requirements
Design Changes to the SZB Instrument Air System

- Selected nuclear safety-related air-operated valves segregated into a new system:
  - Those needed to achieve a safe shutdown state
- **Clean Air Trains System**
  - Two trains, three compressors in each train
  - Increased use of stainless and galvanised steel
  - Dump valves automatically open if air pressure falls below a preset value
  - CATS backed by Nitrogen system
    - so compressors **not** fed from essential boards
Diversity Rules? For SZB Air Systems

• Neither CATS nor Instrument Air System (IAS) were supplied by Essential Boards backed by EDGs
• Most LOOPs of short duration < 2 hours, beyond 24 hours very rare, so CATS is backed up by:
  - N2 system with accumulators
  - N2 Bottles as supplement for key valves
• But no back up for IAS
• Design robust for scenario of Station Black Out, a Design Basis fault for SZB, and enables use of essential control valves in a cooldown of primary circuit to RHR conditions
Low Pressure Nitrogen Storage Tanks
Lessons Learned during SZB Commissioning (1995) and Operation

• During commissioning trials CATS tripped 14 minutes into a “Loss of 11kV” test
  - Sequence of events resulted in a safety valve lifting
• In early winters a temporary diesel-powered compressor backed up IAS
• WANO SOER 1999-01 issued August 1999 on LOOP events
  - Reviewed OE on 25 safety significant LOOP events
  - Included an event at Hunterston B in December 1998
• Mandatory assessment of the SOER performed by SZB (and other UK NPPs)
SZB review of “WANO SOER on LOOP” - Outcome

• Operability after a LOOP needed improving
  - Reduce large burden on operators (MCR and Op Techs)
  - Prevent Pressuriser Relief Tank bursting discs from rupturing, resulting in primary fluid release into containment

• After optioneering, actions were agreed to
  - Replace one compressor in each CATS train with an air-cooled compressor so it did not depend on non-essential water cooling
  - This compressor to be fed from an essential board
  - Transfer some air operated valves, used by operators to retain control of primary circuit, from IAS to CATS
Compressor support systems after modification

**Compressor Unit B & C**
- Intercooler
  - GSW Cooled
- Aftercooler
  - GSW Cooled

415V non-essential supplies

**Compressor Unit A**
- Intercooler
- Motor
- Aftercooler
- Fans fed from 415V essential supplies

415V essential supplies

Fans fed from 415V essential supplies
What followed next

- Safety Category 2 Paper of Intent approved in 2004
  - Operability problems could be primary fluid released into containment
  - Considered to be a significant (but not serious) nuclear safety issue
- Programme of work initiated to modify plant, supported by Safety Case Staged Submissions
- Work overseen by Modification Implementation Meetings
- Work (including Ops handover and training) completed in RF07 (2005)
Now Move Forward to Simulator Studies in 2011

• Operators were aware of a local-to-plant CATS Reset
  - in SOI procedures after LOOP
  - but accepted that this was a design feature, despite the challenge it posed

• PSA team had modified Living PSA to take credit for one compressor in each train being fed by an essential board
  - But were not aware that the CATS compressors needed a Reset after a LOOP

• Requirement then arose to include the local to plant action in the Living PSA, and perform HRA to derive an HEP
Op Tech walks from Operations Plant Office to the first CATS Train "Essential" Compressor Local Control Panel.

Op Tech resets and restarts first CATS Train "Essential" compressor and confirms that it loads up.

CRS Diagnoses the need to reset and restart the CATS "Essential" compressors.

CRS briefs Lead Op Tech to reset and restart the CATS "Essential" compressors.

Op Tech despatched from the Operations Plant Office to reset and restart the CATS "Essential" compressors.

Op Tech phones the MCR to confirm that both CATS "Essential" compressors have been started and are loading.

MCR confirm that the pressures in both CATS Trains are recovering to normal.

Post reactor trip the CRS detects Loss of All 11kV Power and enters the relevant post-trip SOI.

CRS confirms that 3.3 kV Essential Boards 1 & 4 are re-energised and hence determines within the SOI the need to reset and restart CATS "Essential" compressors.

Actions to Restart CATS "Essential" Compressors Post LOOP

Plan 0: Do in order

Plan 1: Do in order

Plan 3: Do in order

1.1 Post reactor trip the CRS detects Loss of All 11kV Power and enters the relevant post-trip SOI

1.2 CRS confirms that 3.3 kV Essential Boards 1 & 4 are re-energised and hence determines within the SOI the need to reset and restart CATS "Essential" compressors

3.1 Op Tech walks from Operations Plant Office to the first CATS Train "Essential" Compressor Local Control Panel.

3.2 Op Tech resets and restarts first CATS Train "Essential" compressor and confirms that it loads up.

3.3 Op Tech walks to second CATS Train "Essential" Compressor Local Control Panel.

3.4 Op Tech resets and restarts second CATS Train "Essential" compressor and confirms that it loads up.

EDF ENERGY
CATS Compressor Local Control Panel
HRA for performing CATS Reset (OSE61)

• First assessed by HEART in 2011: HEP = 0.07
  - But uncertainty over time available (20 minutes) to perform the action
• Then re-assessed using NARA in 2014: HEP = 1.0
  - 1995 Commissioning data:
    - Time to dump valve opening is <15 minutes
  - Simulator OPEX and plant walkdown:
    - Time required >15 minutes
    - Insufficient time => HEP = 1.0
Responding to the Finding

• Safety Case Anomaly raised
  - “Current design places an additional burden on the Op Techs with a high likelihood that they will fail in the task, impairing MCR control of RCS inventory and pressure”

• Review of station arrangements under SOER 1999-1 by a Shift Charge Engineer raised a Condition Report
  - CATS Compressors require a local reset after loss of 11kV. An “unsatisfactory” finding

=> Engineering Change Request raised in priority in 2014
Engineering the Change

• Modification made to the CATS compressors (one per train) supplied from Essential Boards to automate the reset:
  - Reduce the burden on the operator following a LOOP
  - Reduce the risk of a small spillage of reactor coolant to the reactor building

• Straight forward and inexpensive to engineer the change
  - Implementation completed in May 2016 during the last Refuelling Outage (RO14)
LOOP at Millstone in May 2014

• Loss of Instrument Air complicated recovery from a LOOP
  - The sustained loss of IA contributed to rupturing the Pressuriser Relief Tank bursting disc and discharging of 5,760 gallons of water into containment

• The likelihood of an event with similar consequences at SZB has been very much reduced
Response to WANO-SOER 1999-1: Before

- A key statement in the Paper of Intent:
  - [In the original design] “Each CATS train has a back up connection to the nitrogen system, but manual operation would be required for re-pressurisation of CATS”

- This statement is compatible with the original SZB safety case as:
  - Nitrogen system is the back up to CATS after a LOOP
  - CATS is only re-pressurised after Off-site supplies have been restored, and
  - the operators are in recovery mode, and there is no longer a nuclear safety threat
Response to WANO SOER 1999-1: After

• However in the new design:
  - The immediate backup for non nitrogen-backed valves is provided by resetting CATS following load shedding and reloading of the EDGs onto the Essential Boards
  - CATS reset is now required as part of the response to the LOOP, and before the CATS dump valves open
• A very different scenario to the “before” scenario, but the change was not identified in the proposed modification (Paper of Intent)
Human Factors and PSA Aspects

• Action in the “before” scenario was part of recovery from LOOP, not claimed by the LPSA

• In the “after” scenario, the operator action was:
  - Claimed in the LPSA, and graded as LOW,
  - Still needed assessing for feasibility as a local to plant action

• Grade is LOW as LPSA consequences are minor
  - but operators would be keen to avoid RCS spillage in containment
Nitrogen as back-up to CATS in original SZB design

• Benefit
  - Provided a robust defence against SBO
    - an infrequent threat to nuclear safety

• Drawback
  - Sole reliance on nitrogen impaired the response to LOOP
    - a frequent threat to operability and availability

The resolution has finally been achieved by automating the CATS reset operator action at the last outage
How was the Safety Case Anomaly identified?

- Pre-mod trials using simulator in 2001?
  - identified the need for the Operator Reset, but considered it to be consistent with the design
- Simulator studies in 2011
  - with participation of HF and PSA staff
  - but anomaly only raised after manual reset deemed infeasible
- Review of SZB’s mandatory assessment of SOER 1999-1
  - provided independent support to raising mod priority
How might the anomaly have been prevented?

• Had there been a final report following the Paper of Intent and the Stage Submissions:
  - Was the design intent considered to have been met?
  - Has the burden on the operator been reduced?
• Early involvement of Human Factors, starting with the optioneering
  - Would need an understanding of how the change in scenario impacted a low-level plant feature
• Other suggestions are invited
Acknowledgements

- Various skilled staff have helped to make this presentation possible
  - Simulator Tutors
  - Operations Staff
  - PSA and HF Engineers
  - Ex SZB Project Engineers
THANK YOU
Any Questions?
Memo pre Three Mile Island Accident

TMI Shift Supervisor memo: Severe Alarm System Problems

“The alarm system in the control room is so poorly designed that it contributes little in analysis of a causality. Perhaps we can discuss this sometime, preferably before the system, as it is, causes severe problems.”

Edward Frederick
Senior Reactor Operator

Memo 11 months prior to the TMI core melt.